إرشادات دولية مشتركة تكشف دور شركة Integrity Tech الصينية في اختراق الشبكات عالميًا



أصدر المركز الوطني للأمن السيبراني البريطاني وشركاء من ست دول إرشادًا بشأن شركة Integrity Technology Group، يفيد بأنها مكّنت جهات مرتبطة بالصين من اختراق شبكات حول العالم عبر مسح مدعوم بالذكاء الاصطناعي وشبكات botnet واستغلال يدوي.

- الإرشاد موقّع بالاشتراك بين المركز الوطني للأمن السيبراني البريطاني وجهات من أستراليا وكندا واليابان ونيوزيلندا وإسبانيا والولايات المتحدة.
- تُتهم Integrity Tech، وهي شركة صينية ذات صلات حكومية، بدعم جهات تطوّر أدوات وتبيعها وتحصل على بنية تحتية وتستضيفها وتخترق الشبكات.
- يجمع النشاط بين أدوات ذكاء اصطناعي مثل المسح الآلي وشبكات botnet واسعة النطاق واستغلال يدوي لسرقة بيانات سرية، بما في ذلك في قطاعات حيوية.
- النشاط يتسق مع حملات تُعرف أيضًا بأسماء Flax Typhoon وEthereal Panda وRed Juliett.

- يحثّ المركز البريطاني جميع المؤسسات على فهم الأساليب المستخدمة واتباع توصيات التخفيف الواردة في الإرشاد.

نشر المركز الوطني للأمن السيبراني في المملكة المتحدة (NCSC)، التابع لمقر GCHQ، إرشادًا مشتركًا مع ثمانية شركاء دوليين من ست دول. ويوضح الإرشاد كيف مكّنت شركة Integrity Technology Group (Integrity Tech)، وهي شركة صينية لها صلات بالحكومة الصينية، جهات سيبرانية مرتبطة بالصين من استغلال شبكات مؤسسات حول العالم واختراقها.

ما الذي يقوله الإرشاد

وفق المركز، تجمع هذه الجهات بين أدوات الذكاء الاصطناعي، مثل المسح الآلي، وشبكات botnet واسعة النطاق وأساليب استغلال يدوية، بهدف اختراق الشبكات وسرقة بيانات سرية، ومنها بيانات قطاعات حيوية. كما يذكر الإرشاد أن الشركة توظّف أفرادًا يدعمون نشاطًا خبيثًا أوسع، يشمل تطوير أدوات للاستخدام والبيع، والحصول على بنية تحتية واستضافتها، واختراق الشبكات.

ويتسق النشاط المذكور مع حملات معروفة علنًا بأسماء Flax Typhoon وEthereal Panda وRed Julietta وغيرها. وكان المركز وشركاؤه قد كشفوا في سبتمبر 2024 أن Integrity Tech تشغّل شبكة botnet كبيرة استخدمتها مجموعة Flax Typhoon، كما فرضت الحكومة البريطانية عقوبات على الشركة العام الماضي.

لماذا يهمّ ذلك

يؤكد المركز أن اتساع القطاعات المستهدفة يعكس حجم التهديد، وأن على جميع المؤسسات الاطلاع على التحذير والاستفادة من إرشاداته. والإرشاد موقّع بالاشتراك مع جهات من أستراليا وكندا واليابان ونيوزيلندا وإسبانيا والولايات المتحدة، ومتاح على موقع FBI.

ولا يذكر المصدر ضحايا بعينهم ولا ثغرات محددة. لذلك ينبغي لفرق الأمن اعتماد توصيات التخفيف الواردة في الإرشاد مرجعًا أساسيًا ومقارنتها بالضوابط الحالية.

ما يجب فعله الآن

1. احصلوا على الإرشاد المشترك من موقع FBI واطلبوا من فريق الأمن مطابقة توصيات التخفيف مع الضوابط القائمة.
2. تحققوا من أن مصادر استخبارات التهديدات وقواعد الكشف تغطي الحملات المعروفة بأسماء Flax Typhoon وEthereal Panda وRed Julietta.
3. راجعوا انكشاف الأنظمة والأجهزة المتصلة بالإنترنت، نظرًا لاستخدام المسح الآلي وشبكات botnet.
4. فكّروا في تنفيذ صيد استباقي للتهديدات لاكتشاف ثغرات قد لا تظهر عبر المراقبة المعتادة.
5. أطلعوا الإدارة العليا، وأبلغوا عند الاقتضاء عبر قنوات الهيئة الوطنية للأمن السيبراني والجهة التنظيمية القطاعية وفق إجراءات الحوادث لديكم.